PATENT ABSTRACTS OF JAPAN

(11)Publication number : 64-028672

(43)Date of publication of application : 31.01.1989

(51)Int.Cl. G09C 1/00
G06F 15/21
// H04L 9/00

(21)Application number : 62-183278

(22)Date of filing : 24.07.1987

(71)Applicant : HITACHI LTD

(72)Inventor : NAGAI YASUHIKO
TAKARAGI KAZUO
SASAKI RYOICHI

(54) AUTHENTICATION SYSTEM FOR ELECTRONIC TRANSACTION

(57)Abstract:

PURPOSE: To realize the high-speed efficient processing on operation by using a public key for deciphering whose length is shorter than that of an encipherment secret key in an electronic transaction authentication system using a public key encipherment system.

CONSTITUTION: In the processing system where documents are substituted for electric information to perform electronic transactions, data indicating contents of a transaction text is enciphered by the public key encipherment system to generate authentication data. Enciphered authentication data is deciphered by the public key for deciphering to confirm the authentication data. At this time, a public key whose length is longer than that of the encipherment secret key is adopted as the public key for deciphering. A high-speed remainder calculation system using a remainder table is adopted to generate the authentication data. A conventional system where a quotient is obtained and is subtracted from a dividend is adopted to generate the authentication data. Consequently, the speed of the confirmation processing of authentication data is increased because the length of the public key for deciphering is longer than that of the encipherment secret key.